CLAIMS

1. (currently amended) A method of securing data in a computer network and transparently establishing and managing the separation of user-based communities of interest based upon crypto-graphically separated, need to know security levels, said data having one or more security sensitive words, data objects, characters or icons, said computer network having a plurality of computers interconnected together, one of said plurality of computers designated as a data input computer and each of said plurality of computers having a memory therein, ~~a first and a second memory~~ respective memories designated as a remainder store and ~~an extract store~~ respective extract stores in one or more computers of said plurality of computers, said user-based communities of interest representing a plurality of users having a corresponding a plurality of security levels each with a respective security clearance and respective extract store, comprising:

filtering data input from said data input computer and extracting said security sensitive words, data objects, characters or icons from said data to obtain (a) subsets of extracted data and (b) remainder data;

storing said subsets of extracted data and said remainder data in said ~~extract store~~ respective extract stores and said remainder store, respectively; and,

permitting reconstruction of some or all of said data via one or more of said subsets of extracted data and remainder data only in the presence of a predetermined security clearance of said plurality of security levels.

2. (original) A method as claimed in claim 1 wherein said crypto-graphically separated, need to know security levels correspond to respective ones of said plurality of security levels, the method including encrypting said subsets of extracted data with corresponding degrees of encryption associated

with said plurality of security levels, and including decrypting, during the reconstruction, of some or all of said subsets of extracted data only in the presence of said respective security level of said plurality of security levels.

3. (original) A method as claimed in claim 2 including utilizing placeholders in said remainder data representing non-reconstructed, extracted data during the reconstruction, said placeholders being one from the group of characters, icons, substitute words, data objects, underline and blank space.

4. (original) A method as claimed in claim 3 wherein a plurality of placeholders are utilized, said placeholders including characters, icons, substitute words, data objects, underline and blank spaces grouped to represent each respective security level of said plurality of security levels.

5. (original) A method as claimed in claim 1 including defining a plurality of filters, corresponding to said subsets of extracted data, prior to said filtering step.

6. (original) A method as claimed in claim 1 including encrypting said subsets of extracted data and remainder data prior to storing.

7. (original) A method as claimed in claim 6 wherein the step of permitting reconstruction includes decrypting said subsets of extracted data and remainder data.

8. (original) A method as claimed in claim 1 wherein said plurality of computers are configured in a client-server network within which respective computers are designated by respective uniform resource locators (URLs) and said storing utilizes the URL for one or both of said extract store and said remainder store.

9. (original) A method as claimed in claim 1 wherein said plurality of computers are configured in a client-server network within which respective computers are designated by respective uniform resource

locators (URLs) and said data input computer operates as a client in said client-server network and one of said plurality of computers is designated as a server computer, the method including sending said extracted data from said data input computer to said server computer utilizing the respective URL.

10. (original) A method as claimed in claim 9 wherein said step of permitting reconstruction includes downloading said extracted data from said server computer utilizing said respective URL.

11. (original) A method as claimed in claim 1 wherein said plurality of computers are configured in a client-server network within which respective computers are designated by respective uniform resource locators (URLs) and said data input computer operates as a client in said client-server network and one of said plurality of computers is designated as a server computer, the method including sending said extracted data from said data input computer to the computer with said extract store utilizing the respective URL as controlled by said server computer.

12. (original) A method as claimed in claim 10 including the step of encrypting and decrypting said remainder data and extracted data during sending and downloading.

13. (original) A method as claimed in claim 11 including the step of encrypting said extracted data during sending and downloading and decrypting said extracted data during reconstruction.

14. (original) A method as claimed in claim 1 wherein one computer of said plurality of computers includes a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the step of reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays.

15. (original) A method as claimed in claim 1 wherein one computer of said plurality of computers includes a display fed from video memory having a plurality of frame memory segments, and wherein the reconstruction step of the method includes interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments.

16. (original) A method as claimed in claim 1 including deleting said data input from said data input computer after the step of storing.

17. (original) A method as claimed in claim 1 including mapping said storing of said subsets of extracted data with encryption.

18. (original) A method as claimed in claim 1 wherein one of the steps of filtering, storing and permitting reconstruction utilize one of an inference engine, neural network and artificial intelligence process to filter, store and permit reconstruction.

19. (original) A method as claimed in claim 1 wherein said security sensitive data objects are one or more portions of an audio file and the step of reconstruction utilizes extracted data representative of said one or more portions of said audio file.

20. (original) A method as claimed in claim 4 including encrypting said remainder data prior to storing.

21. (original) A method as claimed in claim 20 wherein the step of permitting reconstruction includes decrypting said remainder data.

22. (original) A method as claimed in claim 21 wherein said plurality of computers are configured in a client-server network within which respective computers are designated by respective uniform resource

locators (URLs) and said storing utilizes the URL for one or both of said extract store and said remainder store.

23. (original) A method as claimed in claim 21 wherein said plurality of computers are configured in a client-server network within which respective computers are designated by respective uniform resource locators (URLs) and said data input computer operates as a client in said client-server network and one of said plurality of computers is designated as a server computer, the method including sending said extracted data from said data input computer to the computer with said extract store utilizing the respective URL as controlled by said server computer.

24. (original) A method as claimed in claim 23 including the step of encrypting and decrypting said remainder data and extracted data during sending and downloading.

25. (original) A method as claimed in claim 24 wherein one computer of said plurality of computers includes a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the step of reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays.

26. (original) A method as claimed in claim 24 wherein one computer of said plurality of computers includes a display fed from video memory having a plurality of frame memory segments, and wherein the reconstruction step of the method includes interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments.

27. (original) A method as claimed in claim 24 including deleting said data input from said data input computer after the step of storing.

28. (original) A method as claimed in claim 27 including mapping said storing of said subsets of extracted data with encryption.

29. (currently amended) A computer readable medium containing programming instructions for securing data in a computer network and transparently establishing and managing the separation of user-based communities of interest based upon crypto-graphically separated, need to know security levels, said data having one or more security sensitive words, data objects, characters or icons, said computer network having a plurality of computers interconnected together, one of said plurality of computers designated as a data input computer and each of said plurality of computers having a memory therein, ~~a first and a second memory~~ respective memories designated as a remainder store and ~~an extract store~~ respective extract stores in one or more computers of said plurality of computers, said user-based communities of interest representing a plurality of users having a corresponding a plurality of security levels each with a respective security clearance and respective extract store, the programming instructions comprising:

filtering data input from said data input computer and extracting said security sensitive words, data objects, characters or icons from said data to obtain (a) subsets of extracted data and (b) remainder data;

storing said subsets of extracted data and said remainder data in said ~~extract store~~ respective extract stores and said remainder store, respectively; and,

permitting reconstruction of some or all of said data via one or more of said subsets of extracted data and remainder data only in the presence of a predetermined security clearance of said plurality of security levels.

30. (original) A medium with programming instructions as claimed claim 29 wherein said crypto-graphically separated, need to know security levels correspond to respective ones of said plurality of

security levels, the instructions including encrypting said subsets of extracted data with corresponding degrees of encryption associated with said plurality of security levels, and including decrypting, during the reconstruction, of some or all of said subsets of extracted data only in the presence of said respective security level of said plurality of security levels.

31. (original) A medium with programming instructions as claimed claim 30 including utilizing placeholders in said remainder data representing non-reconstructed, extracted data during the reconstruction, said placeholders being one from the group of characters, icons, substitute words, data objects, underline and blank space.

32. (original) A medium with programming instructions as claimed claim 31 wherein a plurality of placeholders are utilized, said placeholders including characters, icons, substitute words, data objects, underline and blank spaces grouped to represent each respective security level of said plurality of security levels.

33. (original) A medium with programming instructions as claimed claim 29 wherein said plurality of computers are configured in a client-server network within which respective computers are designated by respective uniform resource locators (URLs) and the instructions for said storing utilizes the URL for one or both of said extract store and said remainder store.

34. (original) A medium with programming instructions as claimed claim 29 wherein said plurality of computers are configured in a client-server network within which respective computers are designated by respective uniform resource locators (URLs) and said data input computer operates as a client in said client-server network and one of said plurality of computers is designated as a server computer, the

instructions including sending said extracted data from said data input computer to the computer with said extract store utilizing the respective URL as controlled by said server computer.

35. (original) A medium with programming instructions as claimed claim 34 including encrypting and decrypting said remainder data and extracted data during sending and downloading.

36. (original) A medium with programming instructions as claimed claim 29 including deleting said data input from said data input computer after the step of storing.

37. (original) A medium with programming instructions as claimed claim 29 including mapping said storing of said subsets of extracted data with encryption.

38. (original) A medium with programming instructions as claimed claim 32 including encrypting said remainder data prior to storing.

39. (original) A medium with programming instructions as claimed claim 38 wherein the step of permitting reconstruction includes decrypting said remainder data.

40. (original) A medium with programming instructions as claimed claim 39 wherein said plurality of computers are configured in a client-server network within which respective computers are designated by respective uniform resource locators (URLs) and the instructions for said storing utilizes the URL for one or both of said extract store and said remainder store.

41. (original) A medium with programming instructions as claimed claim 39 wherein said plurality of computers are configured in a client-server network within which respective computers are designated by respective uniform resource locators (URLs) and said data input computer operates as a client in said client-server network and one of said plurality of computers is designated as a server computer, the

instructions including sending said extracted data from said data input computer to the computer with said extract store utilizing the respective URL as controlled by said server computer.

42. (original) A medium with programming instructions as claimed claim 41 including encrypting and decrypting said remainder data and extracted data during sending and downloading.

43. (original) A medium with programming instructions as claimed claim 42 including deleting said data input from said data input computer after the step of storing.

44. (original) A medium with programming instructions as claimed claim 43 including mapping said storing of said subsets of extracted data with encryption.

45. (original) A medium with programming instructions as claimed claim 29 wherein the programming instructions for one of the filtering, storing and permitting reconstruction utilize one of an inference engine, neural network and artificial intelligence process to filter, store and permit reconstruction.

46. (original) A medium with programming instructions as claimed claim 29 wherein said security sensitive data objects are one or more portions of an audio file and the programming instructions for reconstruction utilizes extracted data representative of said one or more portions of said audio file.

47. (currently amended) An information processing system for securing data in a computer network and transparently establishing and managing the separation of user-based communities of interest based upon crypto-graphically separated, need to know security levels, said data having one or more security sensitive words, data objects, characters or icons, said computer network having a plurality of computers for a plurality of users all interconnected together, one of said plurality of computers designated as a data input computer and each of said plurality of computers having a memory therein, ~~a first and a second memory~~ respective memories designated as a remainder store and ~~an extract store~~ respective

extract stores in one or more computers of said plurality of computers, said user-based communities of interest representing said plurality of users having a corresponding a plurality of security levels each with a respective security clearance and respective extract store, comprising:

means for filtering data input from said data input computer and extracting said security sensitive words, data objects, characters or icons from said data to obtain (a) subsets of extracted data and (b) remainder data;

means for storing said subsets of extracted data and said remainder data in said respective extract store and said remainder store, respectively; and,

means for permitting reconstruction of some or all of said data via one or more of said subsets of extracted data and remainder data only in the presence of a predetermined security clearance of said plurality of security levels.

48. (original) An information processing system as claimed in claim 47 wherein said cryptographically separated, need to know security levels correspond to respective ones of said plurality of security levels, the system including means for encrypting said subsets of extracted data with corresponding degrees of encryption associated with said plurality of security levels, and including means for decrypting, during the reconstruction, of some or all of said subsets of extracted data only in the presence of said respective security level of said plurality of security levels.

49. (original) An information processing system as claimed in claim 48 including placeholders in said remainder data representing non-reconstructed, extracted data during the reconstruction, said placeholders being one from the group of characters, icons, substitute words, data objects, underline and blank space.

50. (original) An information processing system as claimed in claim 49 including a plurality of placeholders including characters, icons, substitute words, data objects, underline and blank spaces grouped to represent each respective security level of said plurality of security levels.

51. (original) An information processing system as claimed in claim 47 including means for defining a plurality of filters, corresponding to said subsets of extracted data, prior to said filtering step.

52. (original) An information processing system as claimed in claim 47 including means for encrypting said subsets of extracted data and remainder data prior to storing.

53. (original) An information processing system as claimed in claim 52 wherein said means for permitting reconstruction includes means for decrypting said subsets of extracted data and remainder data.

54. (original) An information processing system as claimed in claim 47 wherein said plurality of computers are configured in a client-server network within which respective computers are designated by respective uniform resource locators (URLs) and said means for storing utilizes the URL for one or both of said extract store and said remainder store.

55. (original) An information processing system as claimed in claim 47 wherein said plurality of computers are configured in a client-server network within which respective computers are designated by respective uniform resource locators (URLs) and said data input computer operates as a client in said client-server network and one of said plurality of computers is designated as a server computer, the system including means for sending said extracted data from said data input computer to the computer with said extract store utilizing the respective URL as controlled by said server computer.

56. (original) An information processing system as claimed in claim 55 including means for encrypting and decrypting said remainder data and extracted data during sending and downloading.

57. (original) An information processing system as claimed in claim 47 wherein one computer of said plurality of computers includes a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the means for reconstruction including means for displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays.

58. (original) An information processing system as claimed in claim 47 wherein one computer of said plurality of computers includes a display fed from video memory having a plurality of frame memory segments, and wherein said means for reconstruction includes means for interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments.

59. (original) An information processing system as claimed in claim 47 including means for deleting said data input from said data input computer after storing.

60. (original) An information processing system as claimed in claim 47 including means for mapping the storing of said subsets of extracted data with encryption.

61. (original) An information processing system as claimed in claim 50 including means for encrypting said remainder data prior to storing.

62. (original) An information processing system as claimed in claim 61 wherein said means for reconstruction includes means for decrypting said remainder data.

63. (original) An information processing system as claimed in claim 62 wherein said plurality of computers are configured in a client-server network within which respective computers are designated by respective uniform resource locators (URLs) and said means for storing utilizes the URL for one or both of said extract store and said remainder store.

64. (original) An information processing system as claimed in claim 62 wherein said plurality of computers are configured in a client-server network within which respective computers are designated by respective uniform resource locators (URLs) and said data input computer operates as a client in said client-server network and one of said plurality of computers is designated as a server computer, the system including means for sending said extracted data from said data input computer to the computer with said extract store utilizing the respective URL as controlled by said server computer.

65. (original) An information processing system as claimed in claim 64 including means for encrypting and decrypting said remainder data and extracted data during sending and downloading.

66. (original) An information processing system as claimed in claim 65 wherein one computer of said plurality of computers includes a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the means for reconstruction including means for displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays.

67. (original) An information processing system as claimed in claim 65 wherein one computer of said plurality of computers includes a display fed from video memory having a plurality of frame memory segments, and the means for reconstruction includes means for interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments.

68. (original) An information processing system as claimed in claim 65 including means for deleting said data input from said data input computer after storing.

69. (original) An information processing system as claimed in claim 68 including means for mapping the storing of said subsets of extracted data with encryption.

70. (original) An information processing system as claimed in claim 47 wherein one of the means for filtering, means for storing and means for permitting reconstruction utilize one of an inference engine, neural network and artificial intelligence process to filter, store and permit reconstruction.

71. (original) An information processing system as claimed in claim 47 wherein said security sensitive data objects are one or more portions of an audio file and said means for reconstruction utilizes extracted data representative of said one or more portions of said audio file.

72. (currently amended) A method of securing data and transparently managing the separation of user-based communities of interest based upon crypto-graphically separated, need to know security levels with a plurality of encryption types, said data having one or more security sensitive words, data objects, characters or icons, said user-based communities of interest representing a plurality of users having a corresponding a plurality of security levels each with a respective security clearance and respective extract stores, comprising:

filtering data and extracting said security sensitive words, data objects, characters or icons from said data to obtain (a) subsets of extracted data for said respective extract stores and (b) remainder data;

encrypting said subsets of extracted data with said plurality of encryption types; and,

permitting reconstruction of some or all of said data via one or more of said subsets of encrypted extracted data and remainder data only in the presence of a predetermined security clearance of said plurality of security levels.

73. (currently amended) A method of securing data and transparently managing the separation of user-based communities of interest based upon crypto-graphically separated, need to know security levels with a plurality of encryption types, said data having one or more security sensitive words,

data objects, characters or icons, said user-based communities of interest representing a plurality of users having a corresponding a plurality of security levels each with a respective security clearance and respective extract stores, comprising:

filtering data and extracting said security sensitive words, data objects, characters or icons from said data to obtain (a) subsets of extracted data for said respective extract stores and (b) remainder data;

encrypting said subsets of extracted data with said plurality of encryption types to obtain multiple level encryption in one document or data object; and,

decrypting all or portions of said one document or data object with multiple level encryption only in the presence of a predetermined security clearance of said plurality of security levels.